

# **Mansfield Solicitors & Advocates Limited, Data Retention and Security Policy**

## **Introduction**

This Policy sets out the obligations of Mansfield Solicitors & Advocates Limited regarding retention of personal data collected, held, and processed by the Firm in accordance with General Data Protection Regulation (“GDPR”).

Mark Chaston shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Firm’s other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Firm has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation; or
- f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Firm and the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Firm’s Data Protection Policy.

## **Aims and Objectives**

The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Firm complies fully with its obligations and the rights of data subjects under the GDPR.

In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Firm, this Policy also aims to improve the speed and efficiency of managing data.

## **Scope**

This Policy applies to all personal data held by the Firm and by third-party data processors processing personal data on the Firm's behalf.

Personal data, as held by the above is stored in the following ways and in the following locations:

- a) The Firm's servers, located in Orpington, Kent, UK;
- b) Azure U.K. South region located in London
- c) Computers permanently located in the Firm's premises at the Orpington office
- d) Laptop computers and other mobile devices provided by the Firm to its employees.
- e) Computers and mobile devices owned by employees, agents, and sub-contractors
- f) Physical records stored in the Orpington office
- g) Paper files are stored with Restore offsite and in the Orpington office

## **Data Subject Rights and Data Integrity**

All personal data held by the Firm is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Firm's Data Protection Policy.

Data subjects are kept fully informed of their rights, of what personal data the Firm holds about them, how that personal data is, and how long the Firm will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

Data subjects are given control over their personal data held by the Firm including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Firm's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling.

## **Technical and Organisational Data Security Measures**

The following technical measures are in place within the Firm to protect the security of personal data:

- a) All emails containing personal data must be encrypted;
- b) All emails containing personal data must be marked "confidential"
- c) Personal data may only be transmitted over secure networks;

- d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using recorded royal mail delivery or courier service;
- h) All personal data transferred physically should be transferred in a suitable container marked "confidential";
- i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Mark Chaston.
- j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely
- k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Firm or not, without authorisation;
- l) Personal data must be handled with care at all times and should not be left unattended or on view;
- m) Computers used to view personal data must always be locked before being left unattended;
- n) No personal data should be stored on any mobile device, whether such device belongs to the Firm or otherwise without the formal written approval of Mark Chaston and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
- o) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Firm where the party in question has agreed to comply fully with the Firm's Data Protection Policy and the GDPR;
- p) All personal data stored electronically should be backed up Daily with backups stored onsite **AND** offsite. All backups should be encrypted;
- q) All electronic copies of personal data should be stored securely using passwords and encryption;
- r) All passwords used to protect personal data should be changed regularly and should must be secure;
- s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.
- t) All software should be kept up-to-date. Security-related updates should be installed not more than 7 days OR as soon as reasonably possible after becoming available;
- u) No software may be installed on any Firm-owned computer or device without approval; and
- v) Where personal data held by the Firm is used for marketing purposes, it shall be the responsibility of Mark Chaston to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

The following organisational measures are in place within the Firm to protect the security of personal data:

- a) All employees and other parties working on behalf of the Firm shall be made fully aware of both their individual responsibilities and the Firm's responsibilities under the GDPR and under the Firm's Data Protection Policy;
- b) Only employees and other parties working on behalf of the Firm that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Firm;
- c) All employees and other parties working on behalf of the Firm handling personal data will be appropriately trained to do so;
- d) All employees and other parties working on behalf of the Firm handling personal data will be appropriately supervised;
- e) All employees and other parties working on behalf of the Firm handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of the Firm handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Firm handling personal data will be bound by contract to comply with the GDPR and the Firm's Data Protection Policy;
- i) All agents, contractors, or other parties working on behalf of the Firm handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Firm arising out of the GDPR and the Firm's Data Protection Policy;
- j) Where any agent, contractor or other party working on behalf of the Firm handling personal data fails in their obligations under the GDPR and/or the Firm's Data Protection Policy, that party shall indemnify and hold harmless the Firm against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## **Data Disposal**

Upon the expiry of the data retention periods set by the Firm, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- a) Personal data stored electronically (including any and all backups thereof) shall be deleted securely Automatically by policies setup in Office 365 Security and Compliance Centre method;
- b) Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely Manually. If it is not viable to remove the data from all the system backups; Should a system data recovery become necessary, the recovered data will be deleted manually once more;
- c) Personal data stored in hardcopy form shall be shredded and professionally disposed of by the Firm's approved supplier.
- d) Special category personal data stored in hardcopy form shall be shredded and professionally disposed of using the Firm's approved supplier.

- e) A Data retention period list will be run monthly by the Financial Controller through our case management system and any records stored in hard form. This list will be provided to the COLP, who will review and confirm to the accounts team the data that should be deleted and or securely destroyed by our data management company. The client case file will then be erased. Only financial transactions will remain however all identifying factors will be removed.

A record of the matter reference number, date matter closed, and date deleted will be recorded.

### **Right to Erasure – “the right to be forgotten”**

When the data subject withdraws consent to holding their data, if the matter is a new business enquiry the details would be passed to the firm’s COLP, who would in turn discuss and pass the information to our Financial Controller who would take steps to erase the data held within our case management system, Proclaim. A GDPR register spreadsheet is saved on the management drive where only the data subject reference number is retained with the deletion date.

If the matter is opened as a client matter on our case management system the data would again be erased from Proclaim, once the COLP has confirmed the same, but the matter number and financial transactions will remain however all identifying factors will be removed.

Any data held in hard format will be securely destroyed by our data management company.

Once the data subject has withdrawn their consent to the holding of their data, they will be advised the only information we shall retain is the reference number should they have a query in the future they wish to discuss with us.

### **Data Retention**

As stated above, and as required by law, the Firm shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in our Data Retention plan.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- a) The objectives and requirements of the Firm;
- b) The type of personal data in question;
- c) The purpose(s) for which the data in question is collected, held, and processed;
- d) The Firm’s legal basis for collecting, holding, and processing that data;
- e) The category or categories of data subject to whom the data relates;

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Firm to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where

such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

In any event the Firm shall carry out an annual review in order to securely delete any personal data which it considers should no longer be retained whether for legal or other business purposes.